UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

An Coolpad cellular telephone, currently in the custody of the FBI, 3600 S. Lake Drive, St. Francis, WI

Case No. 20 MJ 158

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 21, United States Code, Section 841(a)(1)	Distribution of cocaine

The application is based on these facts:

See attached affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

SA

Applicant's signature

FBI SA Jeffrey Baker

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by email and telephone *(specify reliable electronic means).*

Date: 6/1/2020

William E. Duffin

Judge's signature

City and state: Milwaukee, WI

Hon. William E. Duffin, U.S. Magistrate Judge

Printed name and title

Return

Case No.: 20 MJ 158	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jeffrey A. Baker, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device, further described in Attachment A—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent for the Federal Bureau of Investigation (FBI). I have been assigned to the Southeastern Wisconsin Regional Gang Task Force since October of 2017. I have participated in search warrants, investigations, and arrests in which controlled substances and drug paraphernalia were seized. As part of my duties as an FBI Agent, I investigate criminal violations relating to narcotics trafficking offenses and firearms offenses, including criminal violations of the federal laws, including but not limited to Title 21, United States Code, Sections 841, 843, 846, 848, 952 and 963 and Title 18, United States Code, Section 924(c). I have been involved with various electronic surveillance methods, the debriefing of defendants, informants, and witnesses, as well as others who have knowledge of the distribution, transportation, storage, and importation of controlled substances.

3. I have received training in the area of narcotics investigations, violent crime investigations, and the various methods that drug dealers use in an effort to conceal and launder the proceeds of their illicit drug trafficking enterprises.

4. I have participated in investigations that have led to the issuance of search warrants involving violations of the federal narcotics laws. These warrants involved the search

of locations including: residences of targets, their associates and relatives, "stash houses" (houses used as drug/money storage locations), storage facilities, bank safe deposit boxes, cellular/camera phones, and computers. Evidence searched for and recovered in these locations has included controlled substances, records pertaining to the expenditures and profits realized from narcotics trafficking, monetary instruments, and various assets that were purchased with the proceeds of the drug trafficking.

5. This affidavit is based upon my personal knowledge and upon information reported to me by other federal and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

6. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses.

7. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. The property to be searched is a gray Coolpad cellular telephone, with unknown serial number (Device A), recovered during the arrest of Nicholas J WELDON (DOB: September

14th, 1990) on May 15th, 2020, and currently in evidence at the Federal Bureau of Investigation located at 3600 South Lake Drive, Saint Francis, Wisconsin.

9. In February of 2019, case agents initiated an investigation into a group of known and unknown drug traffickers operating in the Milwaukee area, known as the Buffum Meinecke Boys ("BMB"), including, Ramone LOCKE aka "Mone", Amir LOCKE aka "Big Mir", Joey VAZQUEZ aka "Joey", Louis BATES aka "Little Louis", Michael SMITH aka "M&M", Garrell HUGHES aka "Rello", Jesus PUENTES aka "JP", Coury AGEE aka "Lil C", Lamar JOHNSON aka "Fresh", Luis LORENZO aka "Pito", Victor GONZALEZ aka "Bey Bey", and others. As part of the investigation, case agents have interviewed several confidential sources, conducted physical and electronic surveillance, utilized pen registers, reviewed historical phone toll records, reviewed subpoenaed records of documents, and have conducted controlled purchases of cocaine, crack cocaine, and heroin. As a result of the intelligence provided by the confidential sources and the controlled purchases, along with information obtained from other law enforcement techniques, case agents have identified various members of the BMB and identified several sources of supply.

10. On February 19, 2020, a federal grand jury in this district returned an indictment charging multiple subjects associated with the BMB -- including Nicholas J. WELDON, aka "Tick," -- with various controlled substance offenses, Case No. 20-cr-41.

11. On May 15th, 2020, a residential search warrant was executed by the Milwaukee Police Department (MPD) Tactical Enforcement Unit (TEU) at 3259 N 1st Street, in the City and County of Milwaukee, State of Wisconsin. During the execution of this search warrant, Nicholas J. WELDON attempted to escape from the residence via an east facing basement window but was

immediately arrested. A search of the kitchen of the residence by FBI TFO Kody WETZEL revealed: a loaded silver firearm with a black handle, Colt M1991A1, .45 caliber semi-automatic (SN CV08149); a clear plastic baggie that contained pills which field-tested positive for methamphetamine; a blue digital scale with a non-weighable amount of a substance which field-tested positive for cocaine; and a glass Pyrex brand container that contained .49 grams of a substance which field-tested positive for cocaine. In the course of searching the basement, Milwaukee County Sheriff Office (MSCO) TFO Mason KOHLHAPP found Device A, a Coolpad brand cellular telephone on the floor. Device A was in close proximity to the east facing window, where WELDON had recently been.

12. Device A is currently in storage at the Federal Bureau of Investigation. In my training and experience, I know that Device A has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the device first came into the possession of the Milwaukee Police Department and the FBI.

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. *Digital camera*: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. *Portable media player*: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. *GPS*: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. *PDA*: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

14. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications, I know that Device A has capabilities that allows it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

15. Based on my knowledge, training, and experience, I know that electronic devices like Device A can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on such device. This information can sometimes be recovered with forensics tools.

16. There is probable cause to believe that things that were once stored on Device A may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file

system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how Device A was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on Device A because:

a. Data on such storage mediums can provide evidence of a file that was once on the storage mediums but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage mediums that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device like Device A can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is

evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of Device A to human inspection in order to determine whether a particular piece of information is evidence described by the warrant.

19. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

20. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of Device A, as described in Attachment A, to seek the items described in Attachment B.

ATTACHMENT A

The property to be searched ("Device A") is a gray Coolpad brand cellular telephone with an unknown serial number, recovered during the arrest of Nicholas J. WELDON on May 15th, 2020, and currently in evidence at the Federal Bureau of Investigation located at 3600 South Lake Drive, Saint Francis, Wisconsin.

This warrant authorizes the forensic examination of Device A for the purposes of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Target Device described in Attachment A that relate to violations of Title 21, United States Code, Sections 841 and 846, including but not limited to:

   a. lists of customers and related identifying information;

   b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

   c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

   d. any information recording the schedule or travel of Joey VAZQUEZ;

   e. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Target Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet Protocol address to communicate with using the internet including:

   a. records of Internet Protocol addresses used;

   b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.